Technology Strategies for Homeland Security: Adaptation and Coevolution of Offense and Defense

Brian A. Jackson

Terrorists' technology choices are a key part of their ability to create fear in target populations and audiences. Terrorists' interaction with technologies that perform key functions within modern society – e.g., communications or infrastructures – can also be strategies through which they can produce damage and fear. It is the way the terrorist chooses to apply technologies – to cause death and destruction – that sets him apart from the criminal who may be comparably armed and equipped but who uses those technologies for personal or material gain. For homeland security organizations,[1] responses to terrorist threats frequently gravitate toward the use of defensive technical systems. Significant sums of public and private funds have been allocated for development and fielding of security technologies and reduction of societal vulnerabilities. Making good decisions about investments in defensive systems – many of which are costly and intended to reduce the threat of terrorist attack over the long term – requires understanding the interaction between the technology strategies of the terrorist and those of the organizations charged with defending against them.

Technical aspects of the fight between states and non-state groups are frequently portrayed as a discrete interaction between the capabilities of the terrorist and those of the defender. The vehicle bomb is pitted against the perimeter security and any protective blast-resistant features built into its target; the anthrax-containing letter against the detectors in the mail system; the weapon smuggled in hand luggage against the technologies and training of airport security systems and personnel. At the end of this one-on-one interaction between weapon and defense, the attacker and defender step back to see if the terrorist was successful. Drilling deeper, however, makes looking at the fight as a set of discrete interactions appear increasingly artificial. Examination of the technological elements of terrorism invariably highlights the dynamic nature of the problems faced by the defense. The bomb planted by a terrorist group tomorrow will frequently differ from the bomb planted today: the terrorists change the explosive composition, modify the detonator circuitry, and alter the tactics used. The next day, the bomb may be discarded entirely as the group shifts to new attack modes, alternative weapons, and novel tactics.

Some of these adaptations will have nothing to do with the actions taken by the defender, resulting simply from the desire of the terrorists to be more effective or lethal. Detonator modifications may be an attempt to reduce premature explosions that kill only the terrorists. The appearance of a new weapon may simply mean that the group is seizing an opportunity, i.e. through theft, purchase, or gift; the organization obtains a new tool and wants to use it. Frequently, however, terrorists' adaptation has everything to do with the steps taken to defeat them. New remote-control initiators are needed because the defender is jamming the groups' current detonator or standoff weapons are acquired because security measures keep the terrorists away from desirable targets.

The opportunity for each side of the conflict to influence the other means the interaction between them is more complex and much richer than merely a sequential set of discrete clashes – and that defensive planning cannot be approached as if the

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Technology Strategies for Homeland Security: Adaptation and Coevolution of Offense and Defense	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Center for Homeland Defense and Security,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**16**	

terrorism problem can be "solved" if simply the right defensive measure can be crafted and deployed. At the minimum, it is a multi-turn game involving many distinct players, where future clashes are informed by past actions – and by attempts to foresee future actions. But the depth of interaction goes further still: neither side limits its activities to perfecting its own future strategies based on the outcome of previous clashes, but also seeks to shape the environment of its opponent, even in the absence of direct interactions between them.

This bi-directional interaction – the terrorist shaping the environment of the defender and vice versa – can be viewed as a process of *coevolution*.[2] In nature, coevolution is defined as reciprocal changes that occur to species that interact in the same environment. Coevolution occurs between species that compete – e.g., predators and their prey – where changes in one produce selective pressure for changes in the other. In biological processes these changes are genetic and are produced through natural variation, recombination, and selection. Changes arise; those that are beneficial are rewarded with survival and those that are not die out. Similar forces can drive organizational change,[3] with the pressures exerted by each side on the other punishing poor technology or other choices.

It is our argument that thinking about the interaction of terrorist groups and security organizations in these coevolutionary terms is useful, particularly for analysts in organizations charged with designing security approaches and making investments in security technologies. Building on the results of a research effort at RAND focused on terrorists' technology behaviors,[4] we argue that such approach would appear particularly valuable for understanding threats to the performance of counterterrorism technologies, identifying opportunities to shape terrorist behavior in ways that are advantageous for security efforts, and can to help identify more robust and, potentially, less resource intensive approaches for homeland security technology design. In the following sections, we first explore terrorist choices and their implications for defensive thinking, and then transition to considering paths for creating "evolutionarily robust" defensive approaches.

PRESSURE ON THE DEFENDER – TERRORISTS' TECHNOLOGY STRATEGIES

Choices made by terrorists are a primary determinant of the value and success of defensive efforts. Seeking to understand the drivers of terrorist technology strategies and identify likely future adaptations creates long-term challenges for security planning. The nature of terrorist groups poses difficulties for doing so, however. Looking across a range of groups and technologies, three central challenges are apparent:

- Terrorist incentives for adopting or rejecting new technologies are rarely observable or obvious, limiting the ability of planners to predict terrorist innovation trajectories;
- Terrorists have strong incentives to adapt well, and have identified multiple strategies for adaptation; and

- Terrorists confront defensive actions directly, degrading the utility and protective value of those actions.

Terrorists Have Varied Technology Incentives

Among analysts examining terrorist behavior, there is broad acceptance that terrorists adapt and evolve over time, though the forces that shape that adaptation are hardly transparent. This lack of transparency has provoked debate about the incentives for terrorist innovation, with evident uncertainty surrounding paths for future innovation. In considering terrorist weapons choices, many analysts have focused on the utility of novel and advanced weapons to terrorist groups, suggesting there will be enduring incentives for terrorist groups to seek them out and use them.[5] Others point out that most terrorists appear to be "operationally conservative," predominantly using basic technologies like the gun and the bomb, suggesting that incentives for innovation may not be particularly strong.[6] Debates about the current terrorist threat and the potential for terrorist use of advanced or unconventional weapons can be viewed through this lens – where the view of terrorists as innovative or conservative frames assessment of the level of threat.

Though apparently contradicting one another, these two views of terrorist technology decision making do not, in fact, conflict. In selecting what technologies to pursue, terrorists' strategies will undoubtedly be governed by a judgment about how the benefits of a technology compare with what is involved in obtaining it, what risks are associated with doing so, and on how attractive a new technology looks compared with other tactical and technological options available to the group. While terrorist groups may not necessarily think about these decisions in these terms, this decision process can be thought of as involving a comparison of the apparent costs and benefits[7] of acquiring the new technology.[8] Even if that comparison is implicit rather than an explicit, and will almost certainly be based on cost and benefit criteria that are idiosyncratic to the terrorist group, cost/benefit *perceptions* will underlie decision making. In this paper, we will use the language of costs and benefits to think through terrorist decisionmaking, even if actual decisions in groups may not approach anything like a formal comparison and may involve both costs and benefits that are unique to the groups involved. In some situations, the benefit of novelty will outweigh the costs and risks associated with it;[9] in others, "tried and true" technologies will be good enough, particularly if there are many ways to apply those technologies in its operations.

Given the risks inherent to terrorist activities – and the terrorists' desire that operations be successful – there will always be tradeoffs between novel technologies and dependable alternatives. Similar tradeoffs will exist for individual technology choices, where the terrorists' assessment of their costs, benefits, and risks will determine whether the group pursues one weapon over another, uses cellular phones for communication or relies on e-mail, and so on. Differences in the environments of individual groups, or of different factions within the terrorist organization, will shape assessments and determine which technology will be chosen.

As a result, while some generalizations about likely terrorist pathways can be made – e.g., analysts can assess the variety of technologies potentially useful to terrorists, articulate why some might be more attractive than others, and rule out some entirely – many possible paths will always remain. The influence of "wild card" external influences, such as other terrorist groups that willingly act as a source of technologies for others, can shift the apparent costs, benefits and risks of technologies and significantly influence such judgments.[10] Differences in groups' environmental conditions (i.e., factors that shape their decisions about technology acquisition) could therefore produce markedly different outcomes from the perspective of the security planner and make it difficult to put bounds around groups' likely technology strategies.

Terrorists Have Strong Incentives to Adapt Well and Varied Strategies for Doing So

Returning to the evolutionary analogy introduced in the opening of this paper, when they are challenged by strong anti- and counter-terrorism measures, terrorist groups have strong incentives to adapt to maintain their effectiveness and to survive. When faced by a change in its environment, an organization must adapt quickly. When the stakes are high and the change threatens the viability of the organization, speed is critical. To respond quickly, one of two conditions must exist: (1) a group must already have solutions to problems that can be used immediately,[11] or (2) it must develop solutions quickly. Developing solutions rapidly depends on how well the group learns and implements its learning.[12] Groups that learn well can be proactive in shaping their own environment rather than reacting to exogenous change; those that cannot may be unable to adapt fast enough to survive the environmental shift. Looking across groups that have been successful in their learning efforts, we have defined three broad technology strategies representing different combinations of these two elements:[13]

1. Versatility

Versatile technology strategies focus on technologies that are suitable for a wide variety of operational contexts and tactical applications. "Guns and bombs" are examples of technologies that can be used in many different types of operations. Versatile capabilities are therefore transferable if the operations they are currently employed in are denied to the terrorist. This transferability enables rapid adaptation to certain types of environmental change. For example, it has been observed that many predators in nature are generalists to enable facile switching among prey types as environmental conditions shift.[14] However, relying on versatility may limit the ability to adapt in other circumstances as it depends on the availability of substitute targets or operations where the technology is applicable.

2. Specialization

Specialized technology strategies focus on developing high levels of capability in specific areas. Specialization is required to respond to some types of change. For

example, as a result of jamming of radio detonators for their bombs, many terrorist organizations have been forced to make electronic modifications to circumvent the countermeasures. Doing so requires a level of specialized understanding of those systems, and a group without that knowledge could not adapt.[15] Specialization may therefore enable adaptation in circumstances where relying on versatile technologies may fail. However, it may take time – since adaptation may involve "opening up" and altering the technologies that the group is using. Furthermore, specialization requires resource commitments to develop expertise and knowledge. This trade between the benefits of specialization (getting much better at a given task) and the costs (reducing performance for other tasks) can be observed in natural systems as well.[16] Environmental shifts might also eliminate the value of a specialty (e.g., a group that made the choice to specialize in one attack mode would pay a steep price if security measures subsequently made it impossible to use it on desirable targets).[17]

3. Variety

Variety-based technology strategies focus on maintaining a broad range of technology options to draw upon as required. In some cases, variety can be provided to the terrorist group by the market: when a range of commercial technologies for functions like communications are available, terrorists can switch among them as needed. Maintaining other variety can require on-going resource commitments (e.g., maintaining expertise in small-unit armed assault operations), though others may be less resource-intensive (e.g., groups returning to using command wire bombs as alternatives to radio detonation). The choice by a group to be a "jack of all trades" and maintain many different capabilities may limit its ability to develop high levels of expertise in any one area or technology.

Separating technology strategies into categories does not imply that individual terrorist organizations choose only one of these strategies. Large organizations can pursue more than one simultaneously, e.g., training much of the group in versatile technologies while isolated elements are allowed to specialize. Similarly, how the boundaries are drawn around a "technology" matter – e.g., while bombs as an element of operations are a versatile technology pursued by almost all terrorist groups, bomb components may be the focus of specialization activities.

Terrorists Take On the Defense Directly

Though weapons choices are a key part of terrorists' technology strategies, a key driver for adaptive behavior and evolution are the actions taken by the defense. Looking across a variety of terrorist organizations, a similar set of strategies can be identified for how these groups evolve in response to defensive measures:[18]

1. Altering operational practices

By changing the ways it acts or designs its operations, a terrorist group may degrade the value of a security measure. Such changes frequently include efforts

to hide from the technologies. Such options are particularly potent for technologies that must be "triggered" by detection of the terrorist (versus static defenses that are "always on"). The observation of such behaviors in biological systems has resulted in definition of a specific category of coevolution, "information coevolution," capturing the efforts of organisms to hide from others' detection capabilities (and the resulting pressure on the other creatures to heighten those detection capabilities in response.)[19]

2. Making technological changes or substitutions

By modifying its own technologies, acquiring new ones, or substituting new technologies for those in use, a terrorist group may be able to neutralize or circumvent a defense. The wide variety of applicable "off-the-shelf" technologies for many terrorist applications facilitates this strategy.[20]

3. Avoiding the defensive technology

Rather than modifying how it operates, a terrorist group may simply move its operations to an area not covered by the defense. Such displacement changes the distribution of terrorism and, while this may constitute successful protection in the area where the technology is deployed, the ability to shift operations elsewhere limits the influence the technology can have on the overall threat level.[21]

4. Attacking the defensive technology

If appropriate avenues are available, a terrorist group may attempt to destroy or damage a defensive technology. Groups may also attempt to exploit the technology to "turn it against the defender" by creating false alarms to waste resources, tire defenders, or desensitize the system.

Just as the three fundamental offensive technology strategies above constitute a menu from which an organization can build its strategy, groups facing defensive pressures can deploy these strategies in response. Extending the coevolutionary analogy, these mechanisms represent the way the terrorist selectively pressures the defender.

IMPLICATIONS FOR HOMELAND SECURITY TECHNOLOGY STRATEGIES

From the perspective of defensive planning, the variation in terrorists' technology strategies means that homeland security organizations will always face a heterogeneous threat. For any given terrorist cell or group, local influences on costs, benefits, and risks of new technologies will make it difficult to generalize about likely technology strategies. Contemporary shifts in the structures and characteristics of groups – for example, terrorism inspired by broader movements (e.g., global jihadist, radical environmentalism, and others) – reinforce the likelihood of variety in technology decisions as weapon and other technology selections are based on idiosyncratic rationales.[22] For large enough movements, this could produce dynamics not dissimilar

from evolution by natural selection: disaggregated decision making by individual cells producing extremely broad variation in technology strategies, with counterterrorist efforts exerting selective pressure on the results.

Terrorist interaction with defensive measures means that defenders face an additional and varied threat to their own actions and the defender is at a disadvantage. To plan its actions, the defense must attempt to predict the terrorists' responses. Particularly if defensive measures are open to observation,[23] the terrorists need only to wait and craft appropriate countermeasures. The terrorists are largely in control of when they interact with defensive measures – they get "last move advantage." For systems that allow repeated interaction at an acceptable level of risk and, therefore, the chance to test them and experiment with countermeasures, this advantage can be important. There are also asymmetries in resource requirements: defensive actions, particularly for large and populous nations like the United States, are frequently costly and require long lead times. Those costs make attempts to defend everything against every threat untenable, while the terrorists' efforts potentially create a high price for making flawed decisions about how and when to defend specific potential targets.

Given the difficulties posed by terrorists' adaptive behavior, actions to limit such groups' ability to adapt and learn are often one goal of counterterrorism action.[24] Given the breadth of the terrorist threat, it is unlikely that such action will significantly reduce the heterogeneity in the threat faced by defenders. How should homeland security organizations responsible for *defending* the country against terrorism respond to the breadth of terrorists' technology strategies and their capability to evolve over time? Our recent research suggests three possible paths.[25]

1. Focus on defensive strategies that can adapt, therefore making it possible to counter adaptation by terrorist groups.
2. Accept that terrorist organizations adapt over time, and seek to influence the direction of that evolution.
3. Seek strategies where defensive performance is robust in spite of changes in the terrorists' strategy or tactics.

The defender has the freedom to pursue one or more of these options when designing a defensive technology strategy. The following sections examine each path and example strategies.

Designing Defenses That Can Adapt When Necessary

The risk that adversaries will find ways around defensive measures clearly means that technology design efforts should include focused efforts to identify vulnerabilities that might be exploited and address them before the defenses are deployed. However, just as it is impossible to protect every target from every threat, resource constraints mean it is impossible to make every defensive technology impenetrable. As a result, a prudent homeland security technology strategy will recognize the potential for even well-designed defensive technologies to be circumvented. In that case, the burden is pushed back on the defender and reconstituting protection will depend on the *defense's* ability

to learn and adapt. How well it can do so depends in part on the organizations maintaining the defense and the characteristics of the defensive technologies they have installed.

In natural coevolution, how effectively organisms change and respond is framed by how readily they vary, reproduce, pass on valuable traits, and how effectively nature eliminates individuals with poor characteristics. In comparison, organizations can have advantages and disadvantages in the speed and effectiveness of adaptive behavior. Organizations that can spread and implement proven strategies can speed their adaptation, without having to wait for the passage of time or attrition to reinforce good ideas. Conversely, organizations can also choose *not* to change. Bureaucratic friction, inertia, and politics can produce resistance to the spread of advantageous strategies and many organizations lack strong selective pressures to dispassionately drive poor strategies into extinction.[26] As a result, choices and organizational characteristics that limit adaptive ability become disadvantages.

Given that terrorists will seek to learn their way around defensive measures, technology strategies should be designed in a manner that recognizes this goal. This applies both to individual defensive technology systems and defensive technology strategies. If the characteristics of a technology system are essentially fixed, it is a static target for terrorist adaptive efforts and, once circumvented, may produce little defensive benefit. A focus on ways to build adaptability into defensive systems is therefore an absolute necessity. Similar arguments can be made for flexibility in the way organizations carryout their activities – e.g., how information is analyzed and deployed to counter the terrorist threat – to enable adaptation as circumstances change. Shifts in the ways that terrorists are applying technologies, such as the scenarios explored in our analysis of networked information and communications technologies,[27] also will require agility to expand or change defensive technology portfolios in response.

Forces that limit adaptability must also be considered and hedged against. Decisions that necessitate technological "lock in" and static properties will inevitably produce some vulnerability. The challenge in those situations is to manage that vulnerability to keep it within acceptable limits. Beyond the characteristics of specific technologies, choices made in how technologies are produced and used can also create vulnerability. Increasing dependence on individual systems for detection or communication might be problematic, for example, if a terrorist group learned how to deceive, spoof or penetrate the systems. If the capabilities provided by the technologies are woven too tightly into many preparedness and response systems, it might not be possible to "pull the plug" on the systems if they were compromised. The scale of investments made in specific technologies can similarly produce lock-in that constrains future adaptability. If the defense is pushed into making large-scale investments in a few defensive systems, the sunk costs, associated organizational structures, and commitments that coalesce around major programs may foreclose future alternatives. Depending on the nature of the threat, limiting the scale of current investments could be a strategy for preserving flexibility and adaptive agility.

The argument for flexibility can be made both with regard to individual technologies and to expenditures on security in total. Because the commitment of resources to

security is a major impact of terrorism on targeted nations, preserving the flexibility to scale back security expenditures as circumstances warrant is also important. Decisions that lock-in resource commitments produce friction limiting their movement to other areas (whether for security against other threats or to other more productive applications) and, therefore, significantly limit adaptability and agility. In nature, the tradeoff between commitment of energy and resources to defense versus growth/reproduction is particularly brutal – and devoting too much to defenses can produce negative outcomes as certainly as devoting too little. As a result, organisms are observed to "give up" defensive behaviors or traits because of competing selective pressures to grow and reproduce. [28]

Just as use of a "variety" strategy by terrorist groups can help them adapt more rapidly to changing circumstances, having a variety of defensive options and diverse technologies available can provide versatility to the defender. In an extended conflict against a given terrorist organization, the terrorist may eventually overwhelm or circumvent even the most adaptable defensive technology. If and when that occurs, new options will be needed. Given the potential for such "adaptive destruction" of individual security approaches, planning must consider defensive technologies as a portfolio, maintaining possibilities for alternative approaches in the event currently effective technologies are neutralized. Such a strategy should ideally be applied to organizational capabilities broadly, rather than narrowly in the technology realm.[29]

Building such a "palette" of capabilities will rarely be easy. While it may be simple enough to put certain types of technology "on the shelf" to be called upon if needed, capabilities that rely on individuals' specialized expertise are more difficult to maintain. Preserving capabilities that are not currently high profile may also be difficult given pressures to use resources efficiently. However, this is one area where governments potentially have an advantage over non-state adversaries: large government organizations are more likely to have the resources needed to build and maintain a prudent portfolio of capabilities that can be called upon when needed.

Understanding and Seeking to Influence Adversary Evolution

Research on terrorist behaviors has shown that, even when defensive efforts do not fully "shut down" the activities of a terrorist organization, the nature and deployment of defenses strongly influence the perceived costs, benefits, and risk associated with possible courses of action. In response to defensive changes, groups have aborted operations and shifted their attention elsewhere, pursued new weapons procurement efforts, and instituted major security efforts to protect themselves from infiltration and arrest. This ability to influence behavior is at the heart of why an analogy to coevolutionary processes is useful and demonstrates that defenders have leverage to shape terrorist activities.

To adapt and evolve, terrorist organizations have specific needs for information, capabilities, and other resources. If strategies are devised to prevent fulfilling those needs, their ability to adapt effectively can be blunted. For example, security organizations should consider whether the efficacy of a defensive technology hangs on

the ability to "keep secrets" about how it functions, how such secrets might be compromised, and whether a terrorist group could discern them from the outside. Technologies which rely on such approaches can be fragile. Technology designers should also consider whether testing – such as action-reaction challenging by adversary probes – could provide vulnerability data, whether groups willing to sacrifice low-level operatives in exploratory operations against the system can learn how to evade it, and whether the system's characteristics are sufficiently observable that an adversary might see how its capabilities might be saturated and overwhelmed. To the extent that features can be incorporated that defeat or degrade the ability to gather such information, the ability of the technology to deter or defeat terrorist operations will be bolstered.

The defense must also remain cognizant of other changes that might facilitate adaptation. For example, our examination of technology-transfer activities between terrorist groups demonstrated that such interactions can be significant influences on group capabilities and that a variety of incentives exist for groups to interact with one another. New technologies can facilitate group evolution as well. The integration of technical components in weapons systems that reduce the need for training and expertise before the systems can be used effectively could make the systems easier for non-state groups to use and increase their attractiveness. Shaping the incentives of potential knowledge sources is therefore important to limit how readily capabilities can spread among non-state groups. Such strategies do not apply where terrorists have many "commercial technology options," such as information and communications technologies, as the broad availability of these technologies will defeat most attempts at control.

However, the general conservatism observed in most terrorists' choices of weaponry and acceptable levels of operational complexity – i.e., reliance on "tried-and-true" firearms and explosives applied in straightforward ways – suggests a sensitivity to costs and risks that could also be used to shape terrorists' behavior. Traditional counter-proliferation measures and efforts to deter specific types of attacks apply this strategy, seeking to limit the availability of key technologies and weapons, or increase the perceived costs and risks of particular courses of action. Our examination of next-generation conventional weapons suggests opportunities for actions to influence terrorists' calculus about the attractiveness of specific systems.[30] In contrast to weapons they manufacture for themselves, commercial weapons are inherently "black box" technologies for terrorists: without a full understanding of their electronics and other components, the user must trust that the weapons will function as expected. Incorporating technical controls into such weapons (e.g., that provide positional information on the weapon or restrict its functioning to permitted geographic areas through the global positioning system) could increase perceived risks[31] and deter their use. To the extent that such controls can be designed to force terrorists into "all or nothing bets" – the terrorists are uncertain that the weapon will function until it is deployed at the intended target – the deterrent value is likely to be greatest.[32]

Similarly, defensive measures that force terrorists to make focused investments in individual areas can "lock them in" and limit their future options. One advantage the terrorist group has is the ability to walk away from choices that are no longer

advantageous – but, the larger the investment and greater the expertise a group has developed in a specific area, the harder it is to do so. Furthermore, design of defensive technologies that cannot be defeated by a group through a "one time investment" – e.g., even if an adversary develops a countermeasure, implementing it requires ongoing action and commitment of resources – are superior. Depending on the magnitude of its available resources, such a "drag" could constrain the group's violent activities.

Finally, defensive organizations have to foresee, to the extent possible how defensive choices might change the adversaries' future incentives. Paradoxically, a group's efforts to adapt and survive when faced with defensive actions can help it become a more potent threat than before the defenses were deployed. The most basic manifestation of this effect is the selective pressure technologies and other security measures exert on terrorist groups, eliminating the less talented individuals and reducing a group to a hardened core. But defensive measures could also direct terrorists' choices in directions that are negative from the defenders' perspective: if a particular security measure pushes terrorists toward attack modes for which no good defensive options exist, a country might be better off not implementing those measures or doing so only selectively–while pursuing the groups through other means that might be less likely to produce negative adaptation on the terrorists' part. [33] To the extent possible, these later-stage evolutionary pathways should be considered in the design of defensive technologies to ensure that short-term gains in security are not offset by the creation of larger long-term vulnerabilities.

Although the use of defensive measures to shape terrorist behavior could be a useful part of a broad-based homeland security effort, doing so requires that we assess the success and failure of security efforts differently than usual. When used to shape behavior, the goal of technology may not be to prevent every terrorist operation; in some cases technology may explicitly allow certain types of activities by groups as part of an effort to shape their future behavior. From this perspective, "scoring" the conflict between the defender and attacker should not be done based on binary success or failure in preventing individual operations, but on the long-term evolution of terrorist groups and their ability to pose a significant threat to the nation.

Identifying Robust Defensive Strategies

The heterogeneity inherent in the terrorist threat means that homeland security organizations must craft a defensive technology strategy to be robust across a wide threat spectrum, rather than optimized for the threat posed by some particular terrorist group. To the extent that robust solutions can be identified that are not directly tied to the nature or specific characteristics of the threat, defenses will also be less sensitive to any changes individual terrorist groups make that shift the level or type of threat they pose.

Examples of strategies that might provide "cross-resistance" to many threats include the design or retrofitting of fault tolerance and robustness into target systems so that damage will be minimized if attacks are carried out. Similarly, investments in rapid response and repair capabilities to provide resilience if a successful terrorist operation is

carried out provide another option. Such approaches have a number of advantages when viewed with terrorists' technology strategies in mind. Increases in the robustness and resilience of systems can be implemented via changes that fundamentally alter the characteristics of a potential target – e.g., a critical infrastructure network – and it is therefore difficult for the terrorist to counter the system's defensive value. Many such measures may in fact be invisible to terrorist efforts to gather targeting information and may deter attack across the system because of the increased uncertainty in outcome. For example, rapid repair of a damaged bridge, which the terrorist hoped would cause severe disruption in transportation systems, will deny the adversary his intended outcome and significantly reduce the effect on the nation, even if the attack itself is not prevented. In circumstances where the outcomes the terrorists desire can be denied, even without acting against or seeking to disrupt the terrorists' actions directly,[34] the threat posed by the organization can be neutralized without providing it with clear incentives or signals about how to make future attacks more successful.

Beyond general-purpose response strategies, building robustness into defensive strategies can also be achieved by considering individual defensive approaches within an overall "systems view" of homeland security. Though individual defensive approaches may be vulnerable to the counter-technology strategies described above, layered combinations of approaches and measures may be far less so. Implementing this approach requires consideration of the full set of defensive capabilities that can act to defeat or blunt the impact of terrorist action to assess how those capabilities will function as a composite defense. When added together, the effectiveness of defenses should no longer depend on "single links in a chain" – e.g., identification of a suspected terrorist at a border checkpoint or early detection of the release of a biological agent – where successful evasion by the terrorist or a single missed signal negates the value of the entire system. Instead, a focus on how even imperfect performance of multiple layers might reinforce one another and provide successive opportunities to detect and frustrate terrorist action can provide a more fault-tolerant defensive approach.

CONCLUSIONS

Thinking about terrorist and counterterrorist conflicts in a dynamic way is superior to viewing them as single, static engagements between adversaries. However, simply saying such a conflict is dynamic and observing that terrorists adapt and change over time helps security planning only modestly. It is indeed true that terrorist threats are heterogeneous and will shift over time, but planners shouldn't therefore conclude that the answer is that they must protect every target from every conceivable attack mode. Such a strategy would quickly collapse either under weight of the resource levels required or by spreading defenses so thinly that the performance of the entire security effort was put at risk.

In this discussion, we used coevolutionary theory and examples from the natural world to set up a different way to think about such dynamic conflicts. The central advantage of approaching the problem this way is that it helps to break the tendency – particularly in the design of technical systems – of viewing security measures as

"solutions" to particular and static security problems or assuming that a technology that is effective in some part of that problem space now will be effective indefinitely. This sets up different ways of thinking about the efficacy of defensive measures – in terms of the opportunities they provide to shape adversary behavior, the value of defenses being adaptive so they can be retargeted or modified to address changing threats, and the importance of seeking out defensive strategies whose performance is less sensitive to whether terrorist groups evolve or how they do so. Whether pursued singly or in combination, these strategies can each contribute to building overall homeland security policies that are more robust in the face of the "adaptive destruction" threatened by terrorist groups coevolving under the selective pressures those measures exert on them.

Brian A. Jackson is a senior physical scientist and the associate director of the Homeland Security Research Program at the RAND Corporation. His research focuses on the technological aspects of the terrorist threat and design and assessment of homeland security responses. Mr. Jackson can be reached at bjackson@rand.org.

Acknowledgments
The author acknowledges the contributions of other RAND staff members in the overall research effort on which this paper is based. In particular, David Frelinger and Kim Cragin helped to refine the specific ideas and provided valuable input to earlier drafts of the manuscript. The research described in this paper was supported by Contract # W81XWH-05-F-0191 with the Department of Homeland Security, Science and Technology Directorate, Office of Comparative Studies. The views expressed are the author's and do not necessarily reflect the views or policies of the RAND Corporation, DHS, or any of RAND's other research sponsors.

---

[1] We have used the plural of this term to emphasize that many organizations contribute to the terrorism defense mission. We will refer to this constellation of organizations as "homeland security agencies" and generically as the "defense" or "defender" in the fight against terrorist organizations.

[2] See Marjolijn S. Dijksterhuis, et al., "Where Do New Organizational Forms Come From? Management Logics as a Source of Coevolution," *Organization Science* 10, No. 5 (1999): 569-582, or Arie Y. Lewin, et al., "The Coevolution of New Organizational Forms," *Organization Science* 10, No. 5 (1999): 535-550, for examples of these principles applied to organizations.

[3] For example, in interviews with the author, law enforcement and intelligence practitioners have frequently cited the selective effect of counter- and anti-terrorism measures for removing less effective and skillful terrorists.

[4] Brian A. Jackson, et al., *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, MG-481-DHS, RAND Corporation, 2007; Kim Cragin, et al., *Sharing the Dragon's Teeth: Terrorist Groups and the Exchange of New Technologies*, MG-483-DHS, RAND Corporation, 2007; James Bonomo, et al, *Stealing the Sword: Limiting Terrorist Use of Advanced Conventional Weapons*, MG-510-DHS, RAND Corporation, 2007; Bruce Don, et al., *Network*

Technologies for Networked Terrorists: Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations, TR-454-DHS, RAND Corporation, 2007.

[5] See, for example, Brian Michael Jenkins, "High Technology Terrorism and Surrogate War: The Impact of New Technology on Low-Level Violence," RAND Paper 5339 (RAND Corporation, January 1975), 15; J. Bowyer Bell, *The Gun in Politics: An Analysis of Irish Political Conflict, 1916-1986* (New Brunswick, NJ: Transaction Books, 1987), 50.

[6] For example, discussion in Bruce Hoffman, "Change and Continuity in Terrorism," April 17, 2000, http://www.mipt.org/hoffman-ctb.asp.

[7] Including not only financial costs but also time, personnel, and other resources needed for adoption.

[8] For discussion, of costs and benefits from the terrorists' perspective, see Brian A. Jackson, "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption," *Studies in Conflict & Terrorism*, 24, 2001, pp. 183-213.

[9] Advanced weapons like antiaircraft missiles provide a useful example: clearly their value to some groups is sufficient to enable use, though the spotty results gained by doing so emphasize some of the risks of new technologies. See, for example, Marvin B. Schaffer, "The Missile Threat to Civil Aviation," *Terrorism and Political Violence* 10, No.3 (1998): 70-82.

[10] See Kim Cragin, et al., *Sharing the Dragon's Teeth: Terrorist Groups and the Exchange of New Technologies*, MG-483-DHS (RAND Corporation, 2007).

[11] This case is analogous to the observation in biology that organisms may maintain traits that are not currently advantageous, but may become valuable if their circumstances change.

[12] See Brian A. Jackson, *Aptitude for Destruction, Volume 1: Organizational Learning by Terrorist Groups and Its Implications for Combating Terrorism*, MG-331-NIJ (RAND Corporation, 2005); and Brian A. Jackson, et al, *Aptitude for Destruction, Volume 2: Case Studies of Learning in Five Terrorist Groups*, MG-332-NIJ (RAND Corporation, 2005) for a broader discussion of factors shaping group learning capability.

[13] See Brian A. Jackson and David Frelinger, "Rifling Through the Terrorists' Arsenal: Exploring Groups' Weapon Choices and Technology Strategies," *Studies in Conflict & Terrorism*, 31, No. 7 (2008): 583-604, for an empirical look at differences in group weapons technology strategies.

[14] Edmund D. Brodie III and Edmund D. Brodie Jr., "Predator-Prey Arms Races," *BioScience* 49, No. 7 (1999): 557-68.

[15] Similar arguments could be made for terrorists that became specialized in using particular weapons (e.g., mortar experts) or in attacking particular classes of targets (e.g., armed assaults on specific infrastructure targets.)

[16] For example, J.S. Rana, et al., "Costs and benefits of prey specialization in a generalist insect predator" *Journal of Animal Ecology* 71, No. 1 (2002): 15-22.

[17] Specialization by the offense can simplify the field for the defender. Resource investments in specialization lock in the terrorist group to some extent along specific trajectories. For a particular group, knowledge of specialization can make it possible to shape more specific defenses to the group's actions. This therefore exposes a larger fraction of the group's capabilities to risks (that are difficult for the terrorist to predict) and generate disincentives to specialization for some groups.

[18] See discussion in Brian A. Jackson, et al., *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies*, MG-481-DHS (RAND Corporation, 2007).

[19] See Joel Kniskern and Mark D. Rausher, "Two Modes of Host-Enemy Coevolution," *Popul Ecol* 43 (2001): 3-14, for discussion of information coevolution.

[20] Bruce Don, et al., *Network Technologies for Networked Terrorists: Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations*, TR-454-DHS (RAND

Corporation, 2007). The potential for novel weapons to provide technological opportunities for substitution in response to defenses is also relevant. James Bonomo, et al, *Stealing the Sword: Limiting Terrorist Use of Advanced Conventional Weapons*, MG-510-DHS (RAND Corporation, 2007).

[21] Enders and Sandler have done comprehensive analyses of such behavior for transnational terrorism including displacement effects among target classes. Walter Enders and Todd Sandler, "What Do We Know About the Substitution Effect in Transnational Terrorism?" in Andrew Silke, ed., *Research on Terrorism: Trends, Achievements and Failures* (London, England: Frank Cass, 2004), 119-137.

[22] See Brian .A. Jackson, "Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and Its Application to al Qaeda," *Studies in Conflict and Terrorism* 29 (2006): 241-262, for discussion of a classification scheme for terrorist organizations applicable to their technology decision making and strategy development.

[23] This creates dynamics on the defensive side regarding how much is revealed and obscured regarding the nature and functioning of defensive measures. To the extent that such secrets can be kept, terrorist learning – and this particular component of the threat – can be blunted or delayed.

[24] See Brian A. Jackson, *Aptitude for Destruction, Volume 1: Organizational Learning by Terrorist Groups and Its Implications for Combating Terrorism*, MG-331-NIJ (RAND Corporation, 2005) for additional discussion of targeting groups learning activities as part of counterterrorist efforts.

[25] Emphasizing the relevance of lessons learned from past defense planning, these principles echo the results of some examinations of national defense policy after the Cold War. See, for example, Paul K. Davis, et al., "Adaptiveness in National Defense: The Basis of a New Framework," RAND Corporation Issue Paper (RAND Corporation, August 1996).

[26] In contrast to the real selective pressure that counterterrorist efforts exert on terrorist organizations and their members – providing mechanisms where poor strategies are indeed eliminated through arrest or attrition.

[27] Bruce Don, et al., *Network Technologies for Networked Terrorists: Assessing the Value of Information and Communication Technologies to Modern Terrorist Organizations*, TR-454-DHS (RAND Corporation, 2007).

[28] See, for example, Daniel A. Herms and William J. Mattson, "The Dilemma of Plants: To Grow or Defend," *The Quarterly Review of Biology*, 67:3, 1992, pp. 283-335 or Abrams, Peter and Hiroyuki Matsuda, "Effects of Adaptive Predatory and Anti-Predatory Behaviour in a Two-Prey—One-Predator System," *Evolutionary Ecology*, 7:3, 1993, pp. 312-326.

[29] For example, maintaining capability in a variety of intelligence collection and analysis techniques is valuable, even if only a subset of them are high value at a given time. As circumstances change, techniques that are currently not applicable may become important as terrorist behavior changes or new intelligence data sources become available.

[30] James Bonomo, et al, *Stealing the Sword: Limiting Terrorist Use of Advanced Conventional Weapons*, MG-510-DHS (RAND Corporation, 2007).

[31] Both to the effective functioning of the weapon (and, therefore, risk to the success of any operation in which it was used) and security risks to the organization overall through the potential for tracking the weapons.

[32] Such arguments similarly apply to defensive measures more broadly, not just those related to controlling the use of advanced weaponry.

[33] For example, for a notional terrorist group, the broad implementation of defensive measures against the use of small explosive devices could produce a strong pressure to adopt vehicle bombs to reconstitute the group's ability to strike attractive targets. Since the use of vehicle bombs would significantly increase the group's destructive capability and could be more difficult to counter, it might be a better defensive strategy to either not deploy the defenses or do so at only the most vulnerable targets (thereby reducing

the evolutionary pressure on the group to seek out alternative attack modes), while focusing resources to pursing the group's members through law enforcement action. Though law enforcement action aimed at a group would produce evolutionary pressures of its own, those pressures might be less likely to move the group towards more destructive attack types.

[34] Such an approach could be termed building in asymmetry into defensive measures where advantage is preserved for the defender across a range of possible attack options and scenarios. Such strategies are also attractive because they can provide robustness and resilience against threats that have nothing to do with terrorism – e.g., robustness of electricity infrastructures to outages produced by storms or natural disasters – and therefore produce benefit streams to the defender irrespective of the realized terrorist threat environment.